PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-326693
(43)Date of publication of application : 22.11.2001

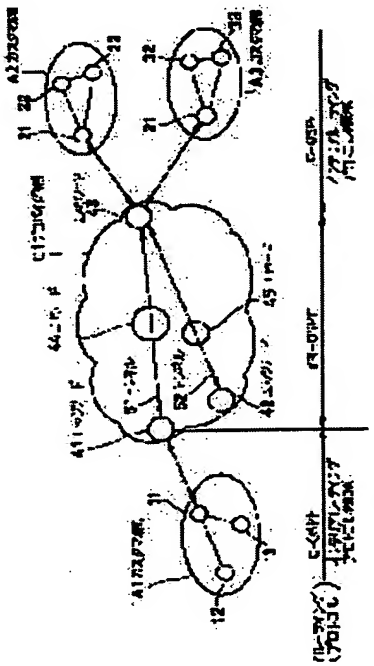
(51)Int.Cl. H04L 12/66
H04L 12/56
H04L 12/22

(21)Application number : 2000-144234
(22)Date of filing : 17.05.2000

(71)Applicant : NEC CORP
(72)Inventor : KAWAKAMI HIROYUKI

(54) COMMUNICATION SYSTEM AND METHOD FOR CONTROLLING COMMUNICATION, AND CONTROL PROGRAM RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a communication unit in which the installation of a BGP is not required for a customer communication unit and for an edge communication unit at a border between a customer network and a provider network, to prevent a load from being increased and, to provide a communication system that uses the communication unit.
SOLUTION: In a virtual private network(VPN), consisting of customer networks A1-A4 and a provider network C1 utilizing tunneling technology, a function for terminating IGPs(Interior Gateway Protocols) in the customer networks is provided to edge nodes 41-43 placed at the border between the customer networks and the provider network. Thus, the installation of the BGP(Border Gateway Protocol) is not required with respect to customer nodes and to the edge nodes, at the border between the customer networks and the provider network.



LEGAL STATUS

[Date of request for examination] 13.04.2001
[Date of sending the examiner's decision of rejection] 12.10.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－326693
（P2001－326693A）
(43)公開日　平成13年11月22日(2001.11.22)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ　５Ｋ０３０
12/56			１０２Ａ
12/22		11/26	

審査請求　有　　請求項の数25　ＯＬ　（全 14 頁）

(21)出願番号　特願2000－144234(P2000－144234)

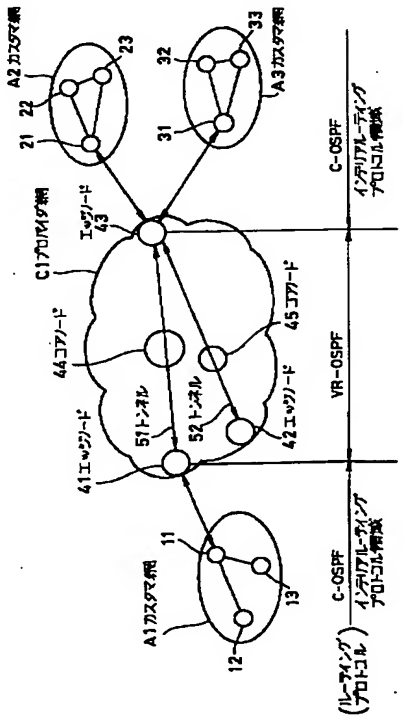
(22)出願日　平成12年５月17日(2000.5.17)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　川上　弘幸
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100088812
弁理士　▲柳▼川　信

Ｆターム(参考)　5K030 GA04 GA11 HA08 HC01 HD03 HD06 LA08 LB20

(54)【発明の名称】　通信装置及び通信制御方法並びに制御プログラム記録媒体

(57)【要約】
【課題】　カスタマ網とプロバイダ網との境界においてカスタマ通信装置とエッジ通信装置とに対してＢＧＰの実装を不要として、負荷の増大を防止した通信装置及びそれを使用した通信システムを得る。
【解決手段】　複数のカスタマ網Ａ１～Ａ３と、トンネル化技術を利用したプロバイダ網Ｃ１からなるＶＰＮにおいて、カスタマ網とプロバイダ網との境界に位置するエッジノード４１～４３に、カスタマ網内のＩＧＰｓ（Interior GatewayProtocols）を終端する機能を設ける。これにより、カスタマ網とプロバイダ網との境界においてカスタマノードとエッジノードとに対して、ＢＧＰ（Border Gateway Protocol ）の実装が不要となる。



【特許請求の範囲】

【請求項１】　プロバイダ網上にトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線（ＶＰＮ）を構築するようにした通信システムにおいて、前記トンネルの入出力端に接続されたエッジ通信装置であって、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端手段を含むことを特徴とするエッジ通信装置。

【請求項２】　前記仮想専用線に関するＶＰＮ構築情報と、前記プロバイダ網に接続され予めカプセルアドレスが割り当てられたポートと前記カスタマ網側の各通信装置のＩＰアドレスとの対応情報とからなるテーブルを更に含み、

前記終端手段は、前記カスタマ網から入力されたパケットの宛先アドレスから前記テーブルを検索する検索手段と、この検索されたカプセルアドレスを基に前記パケットをカプセル化して前記プロバイダ網へ送出するカプセル化手段とを有することを特徴とする請求項１記載のエッジ通信装置。

【請求項３】　前記カプセル化手段は、同一の仮想専用線に属する他のカスタマ網に対して、前記カプセルアドレスを基に前記制御パケットをカプセル化して送出するようにしたことを特徴とする請求項２記載のエッジ通信装置。

【請求項４】　前記終端手段は、前記カスタマ網内のＩＰアドレスの追加やトポロジの変化に応答して前記カスタマ網で生成される制御パケットを受信解読する手段と、この解読結果に従って前記テーブルのデータ更新を行う手段とを有することを特徴とする請求項２または３記載のエッジ通信装置。

【請求項５】　前記終端手段は、前記プロバイダ網から自装置に到着したパケットに対して前記カプセルアドレスが含まれるカプセルを外し、当該パケットに含まれる宛先ＩＰアドレスを基に前記テーブルから送出先を決定して送出する手段を有することを特徴とする請求項２～４いずれか記載のエッジ通信装置。

【請求項６】　前記終端手段は、前記カスタマ網に対する現用インタフェースの障害に応答してこの障害インタフェースに関連する前記テーブル内の情報を削除すると共に、関連する他のエッジ通信装置へ障害通知及び予備インタフェースの通知をなす手段を有することを特徴とする請求項２～５いずれか記載のエッジ通信装置。

【請求項７】　前記終端手段は、他のエッジ通信装置からの障害通知に応答して前記障害インタフェースに関連する前記テーブル内の情報を削除すると共に、前記予備インタフェースの通知に応答して前記テーブル内にこの予備インタフェースに関連する情報を追加する手段を有することを特徴とする請求項６記載のエッジ通信装置。

【請求項８】　前記カスタマ網内で使用されるルーティングプロトコルは、ＯＳＰＦ（Open Shortest Path First）プロトコルであることを特徴とする請求項１～７いずれか記載のエッジ通信装置。

【請求項９】　プロバイダ網上におけるエッジ通信装置間にてトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線（ＶＰＮ）を構築するようにした通信システムにおける通信制御方法であって、前記エッジ通信装置において、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端ステップを含むことを特徴とする通信制御方法。

【請求項１０】　前記エッジ通信装置には、前記仮想専用線に関するＶＰＮ構築情報と、前記プロバイダ網に接続され予めカプセルアドレスが割り当てられたポートと前記カスタマ網側の各通信装置のＩＰアドレスとの対応情報とからなるテーブルが設けられており、

前記終端ステップは、前記カスタマ網から入力されたパケットの宛先アドレスから前記テーブルを検索する検索ステップと、この検索されたカプセルアドレスを基に前記パケットをカプセル化して前記プロバイダ網へ送出するカプセル化ステップとを有することを特徴とする請求項９記載の通信制御方法。

【請求項１１】　前記カプセル化ステップは、同一の仮想専用線に属する他のカスタマ網に対して前記カプセルアドレスを基に前記制御パケットをカプセル化して送出するようにしたことを特徴とする請求項１０記載の通信制御方法。

【請求項１２】　前記終端ステップは、前記プロバイダ網から自装置に到着したパケットに対して前記カプセルアドレスが含まれるカプセルを外し、当該パケットに含まれる宛先ＩＰアドレスを基に前記テーブルから送出先を決定して送出するステップを有することを特徴とする請求項１０または１１記載の通信制御方法。

【請求項１３】　前記終端ステップは、前記カスタマ網内のＩＰアドレスの追加やトポロジの変化に応答して前記カスタマ網で生成される制御パケットを受信解読するステップと、この解読結果に従って前記テーブルのデータ更新を行うステップとを有することを特徴とする請求項１０～１２いずれか記載の通信制御方法。

【請求項１４】　前記終端ステップは、前記カスタマ網との現用インタフェースの障害に応答してこの障害インタフェースに関連する前記テーブル内の情報を削除すると共に、関連する他のエッジ通信装置へ障害通知及び予備インタフェースの通知をなすステップを有することを特徴とする請求項１０～１３いずれか記載の通信制御方法。

【請求項１５】　前記終端ステップは、他のエッジ通信装置からの障害通知に応答して前記障害インタフェースに関連する前記テーブル内の情報を削除すると共に、前記予備インタフェースの通知に応答して前記テーブル内にこの予備インタフェースに関連する情報を追加するステップを有することを特徴とする請求項１４記載の通信

制御方法。

【請求項１６】　前記カスタマ網内で使用されるルーティングプロトコルは、ＯＳＰＦ（Open Shortest Path First）プロトコルであることを特徴とする請求項９～１５いずれか記載の通信制御方法。

【請求項１７】　前記テーブルを集中管理する集中処理装置が設けられており、前記制御パケットの解読結果に従って前記テーブルのデータ更新後に、この更新されたテーブルを前記集中処理装置へアップロードするステップと、前記集中処理装置からこのアップロードされたテーブルを関連するエッジ通信装置にダウンロードするステップとを含むことを特徴とする請求項１３記載の通信制御方法。

【請求項１８】　プロバイダ網上におけるエッジ通信装置間にてトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線（ＶＰＮ）を構築するようにした通信システムにおける通信制御方法のプログラムを記録した記録媒体であって、

前記プログラムは、前記エッジ通信装置において、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端ステップを含むことを特徴とする記録媒体。

【請求項１９】　前記エッジ通信装置には、前記仮想専用線に関するＶＰＮ構築情報と、前記プロバイダ網に接続され予めカプセルアドレスが割り当てられたポートと前記カスタマ網側の各通信装置のＩＰアドレスとの対応情報とからなるテーブルが設けられており、

前記終端ステップは、前記カスタマ網から入力されたパケットの宛先アドレスから前記テーブルを検索する検索ステップと、この検索されたカプセルアドレスを基に前記パケットをカプセル化して前記プロバイダ網へ送出するカプセル化ステップとを有することを特徴とする請求項１８記載の記録媒体。

【請求項２０】　前記カプセル化ステップは、同一の仮想専用線に属する他のカスタマ網に対して前記カプセルアドレスを基に前記制御パケットをカプセル化して送出するようにしたことを特徴とする請求項１９記載の記録媒体。

【請求項２１】　前記終端ステップは、前記プロバイダ網から自装置に到着したパケットに対して前記カプセルアドレスが含まれるカプセルを外し、当該パケットに含まれる宛先ＩＰアドレスを基に前記テーブルから送出先を決定して送出するステップを有することを特徴とする請求項１９または２０記載の記録媒体。

【請求項２２】　前記終端ステップは、前記カスタマ網内のＩＰアドレスの追加やトポロジの変化に応答して前記カスタマ網で生成される制御パケットを受信解読するステップと、この解読結果に従って前記テーブルのデータ更新を行うステップとを有することを特徴とする請求項１９～２１いずれか記載の記録媒体。

【請求項２３】　前記終端ステップは、前記カスタマ網に対する現用インタフェースの障害に応答してこの障害インタフェースに関連する前記テーブル内の情報を削除すると共に、関連する他のエッジ通信装置へ障害通知及び予備インタフェースの通知をなすステップを有することを特徴とする請求項１９～２２いずれか記載の記録媒体。

【請求項２４】　前記終端ステップは、他のエッジ通信装置からの障害通知に応答して前記障害インタフェースに関連する前記テーブル内の情報を削除すると共に、前記予備インタフェースの通知に応答して前記テーブル内にこの予備インタフェースに関連する情報を追加するステップを有することを特徴とする請求項２３記載の記録媒体。

【請求項２５】　前記カスタマ網内で使用されるルーティングプロトコルは、ＯＳＰＦ（Open Shortest Path First）プロトコルであることを特徴とする請求項１８～２４いずれか記載の記録媒体。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は通信装置及び通信制御方法並びに制御プログラム記録媒体に関し、特にプロバイダ網上にトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線（ＶＰＮ）を構築するようにした通信方式に関するものである。

【０００２】

【従来の技術】カプセル化技術を用いたＶＰＮ（Virtual Private Network）構築技術に関して、シスコ（Cisco）社から、プロバイダ網にＭＰＬＳ（Multi Protocol LabelSwitch）を用いた通信方式が提案されている。この様なＶＰＮ技術について説明する。ＶＰＮとは、インターネット等の公衆通信網上で、論理的なグループを形成し、かつそのグループ間で閉域性を保つ機能を設けたネットワークをいう。このインターネット等の公衆通信網には、通常不特定多数のユーザが接続しており、そのために基本的には特定のユーザだけの通信はできず、第三者による不正アクセスは避けられないというセキュリティ上の問題がある。

【０００３】そこで、近年エンドーエンドでセキュリティ対策を施すことにより、インターネット上に仮想的に専用線を構築し、ＬＡＮ（Local Area Netwok）間接続の基幹回線として利用するＶＰＮ技術が注目されている。具体的には、エンドーエンドでのデータの暗号化、ユーザ認証及びアクセス制御等のセキュリティを施した上で、特定の拠点間をインターネットを介して接続し、閉域性のあるグループを提供するものである。

【０００４】かかるＶＰＮを公衆通信網上に実現することで、特定ユーザだけの通信が可能となり、インターネット等を仮想的な専用網として利用することができるのである。この様なＶＰＮ方式に関しては、特開平１０－７０５６６号公報、特開平１１－３５５２７２号公報等

に開示のものがある。

【０００５】図１６はこの様なＶＰＮを使用した通信システムの概略ブロック図である。図１６において、ＬＡＮ等の閉域性のあるグループであるカスタマ網Ａ１～Ａ３と、インターネット等のプロバイダ網Ｃ１とがある。カスタマ網Ａ１はカスタマ通信装置（以下、通信装置のことを単にノードと称する）１１～１３を有しており、また、カスタマ網Ａ２はカスタマノード２１～２３を有しており、更にカスタマ網Ａ３はカスタマノード３１～３３を有している。そして、プロバイダ網Ｃ１には、カスタマ網との境界にエッジノード４１～４３が設けられており、境界以外にはコアノード４４，４５が設けられている。尚、図１６では、カスタマ網Ａ１との境界にエッジノード４１が、カスタマ網Ａ２，Ａ３との境界にエッジノード４２が、それぞれ設けられているものとする。

【０００６】この場合、カスタマ網Ａ１とＡ２，Ａ３との間の通信は、エッジノード間に構築されたトンネル５１により形成されたＶＰＮによって行われるが、このときのルーティングのためのプロトコルの関係は図示のようになっている。すなわち、ＬＡＮ等のカスタマ網Ａ１～Ａ３では、インテリアルーティングプロトコルであるＩＧＰ（Interior Gateway Protocol ）が用いられ、プロバイダ網Ｃ１では、ＩＢＧＰ（Interior Border Gateway Protocol）が用いられ、これ等網間のインタフェース部分では、ＥＢＧＰ（Exterior Border Gateway Protocol）が用いらる。

【０００７】

【発明が解決しようとする課題】従来のＶＰＮ通信方式の問題点としては、図１６に示したＬＡＮ等の閉域性のあるグループであるカスタマ網Ａ１～Ａ３と、インターネット等のプロバイダ網Ｃ１との境界では、ＥＢＧＰが使用されているので、カスタマノードとエッジノードとに対してＢＧＰ（Border Gateway Protocol ）による通信ができるように設定する必要がある。これは、カスタマノードにＢＧＰを実装する必要があるばかりではなく、サービスを受けるカスタマがＢＧＰの知識が必要となり、負荷の増大を招くという欠点がある。

【０００８】また、このようなＶＰＮ方式では、カスタマ網とプロバイダ網との境界でＥＢＧＰが使用されているので、カスタマ網とプロバイダ網との間で、いわゆるマルチホーミング構成を構築することができない。従って、例えば、帰属するエッジノードが停止した場合や、帰属するインタフェース部分にリンク断が生じた場合には、配下のカスタマ網の通信停止を引き起こし、信頼性の低下につながるという欠点がある。

【０００９】更に、プロバイダ網であるＭＰＬＳ網をプロバイダ網Ｃ１内部でＶＰＮ毎の経路情報がＢＧＰで伝達されるので、カスタマ網内で使用されるルーティングプロトコルであるＯＳＰＦ（Open Shortest Path First）のＯＳＰＦ情報が透過的に通らず、結果としてＯＳＰＦドメインが分断されることになる。特に、ＡＴＭ（非同期通信モード）やＦＲ（フレームリレー）を使用した専用線上でＩＰ網を構築する方式のように、単一のＯＳＰＦドメインで各カスタマ網を接続する重要性は極めて大きいにもかかわらず、、図１６の方式では、ＯＳＰＦドメインが分断されてしまうので、単一のＯＳＰＦドメインで各カスタマ網を接続することができないという欠点もある。

【００１０】本発明の目的は、カスタマ網とプロバイダ網との境界においてカスタマノードとエッジノードとに対してＢＧＰの実装を不要として、負荷の増大を防止した通信装置及び通信制御方法並びにその制御プログラムの記録媒体を提供することである。

【００１１】本発明の他の目的は、カスタマ網とプロバイダ網との間でのマルチホーミングを構築可能として、信頼性の向上を図った通信装置及び通信制御方法並びにその制御プログラムの記録媒体を提供することである。

【００１２】本発明の更に他の目的は、ＯＳＰＦドメインが分断されてしまうことをなくして、単一のＯＳＰＦドメインで各カスタマ網を接続することが可能な通信装置及び通信制御方法並びにその制御プログラムの記録媒体を提供することである。

【００１３】

【課題を解決するための手段】本発明によれば、プロバイダ網上にトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線（ＶＰＮ）を構築するようにした通信システムにおいて、前記トンネルの入出力端に接続されたエッジ通信装置であって、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端手段を含むことを特徴とするエッジ通信装置が得られる。

【００１４】そして、前記仮想専用線に関するＶＰＮ構築情報と、前記プロバイダ網に接続され予めカプセルアドレスが割り当てられたポートと前記カスタマ網側の各通信装置のＩＰアドレスとの対応情報とからなるテーブルを更に含み、前記終端手段は、前記カスタマ網から入力されたパケットの宛先アドレスから前記テーブルを検索する検索手段と、この検索されたカプセルアドレスを基に前記パケットをカプセル化して前記プロバイダ網へ送出するカプセル化手段とを有することを特徴とする。

【００１５】また、前記終端手段は、前記カスタマ網内のＩＰアドレスの追加やトポロジの変化に応答して前記カスタマ網で生成される制御パケットを受信解読する手段と、この解読結果に従って前記テーブルのデータ更新を行う手段とを有することを特徴とし、前記カプセル化手段は、同一の仮想専用線に属する他のカスタマ網に対して、前記カプセルアドレスを基に前記制御パケットをカプセル化して送出するようにしたことを特徴とする。

【００１６】更に、前記終端手段は、前記プロバイダ網

から自装置に到着したパケットに対して前記カプセルアドレスが含まれるカプセルを外し、当該パケットに含まれる宛先ＩＰアドレスを基に前記テーブルから送出先を決定して送出する手段を有することを特徴とし、また前記終端手段は、前記カスタマ網に対する現用インタフェースの障害に応答してこの障害インタフェースに関連する前記テーブル内の情報を削除すると共に、関連する他のエッジ通信装置へ障害通知及び予備インタフェースの通知をなす手段を有することを特徴とする。

【００１７】更にはまた、前記終端手段は、他のエッジ通信装置からの障害通知に応答して前記障害インタフェースに関連する前記テーブル内の情報を削除すると共に、前記予備インタフェースの通知に応答して前記テーブル内にこの予備インタフェースに関連する情報を追加する手段を有することを特徴とし、前記カスタマ網内で使用されるルーティングプロトコルは、ＯＳＰＦプロトコルであることを特徴とする。

【００１８】本発明によれば、プロバイダ網上におけるエッジ通信装置間にてトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線（ＶＰＮ）を構築するようにした通信システムにおける通信制御方法であって、前記エッジ通信装置において、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端ステップを含むことを特徴とする通信制御方法が得られる。

【００１９】そして、前記エッジ通信装置には、前記仮想専用線に関するＶＰＮ構築情報と、前記プロバイダ網に接続され予めカプセルアドレスが割り当てられたポートと前記カスタマ網側の各通信装置のＩＰアドレスとの対応情報とからなるテーブルが設けられており、前記終端ステップは、前記カスタマ網から入力されたパケットの宛先アドレスから前記テーブルを検索する検索ステップと、この検索されたカプセルアドレスを基に前記パケットをカプセル化して前記プロバイダ網へ送出するカプセル化ステップとを有することを特徴とする。

【００２０】また、前記終端ステップは、前記カスタマ網内のＩＰアドレスの追加やトポロジの変化に応答して前記カスタマ網で生成される制御パケットを受信解読するステップと、この解読結果に従って前記テーブルのデータ更新を行うステップとを有することを特徴とし、更に前記カプセル化ステップは、同一の仮想専用線に属する他のカスタマ網に対して前記カプセルアドレスを基に前記制御パケットをカプセル化して送出するようにしたことを特徴とする。

【００２１】更にはまた、前記終端ステップは、前記プロバイダ網から自装置に到着したパケットに対して前記カプセルアドレスが含まれるカプセルを外し、当該パケットに含まれる宛先ＩＰアドレスを基に前記テーブルから送出先を決定して送出するステップを有することを特徴とし、また前記終端ステップは、前記カスタマ網との現用インタフェースの障害に応答してこの障害インタフェースに関連する前記テーブル内の情報を削除すると共に、関連する他のエッジ通信装置へ障害通知及び予備インタフェースの通知をなすステップを有することを特徴とする。

【００２２】更に、前記終端ステップは、他のエッジ通信装置からの障害通知に応答して前記障害インタフェースに関連する前記テーブル内の情報を削除すると共に、前記予備インタフェースの通知に応答して前記テーブル内にこの予備インタフェースに関連する情報を追加するステップを有することを特徴とする。また、前記テーブルを集中管理する集中処理装置が設けられており、前記制御パケットの解読結果に従って前記テーブルのデータ更新後に、この更新されたテーブルを前記集中処理装置へアップロードするステップと、前記集中処理装置からこのアップロードされたテーブルを関連するエッジ通信装置にダウンロードするステップとを含むことを特徴とする。

【００２３】本発明によれば、プロバイダ網上におけるエッジ通信装置間にてトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線（ＶＰＮ）を構築するようにした通信システムにおける通信制御方法のプログラムを記録した記録媒体であって、前記プログラムは、前記エッジ通信装置において、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端ステップを含むことを特徴とする記録媒体が得られる。

【００２４】本発明の作用を述べる。プロバイダ網とカスタマ網との境界に位置するエッジ通信装置において、カスタマ網でのルーティングプロトコルを終端する構成とする。これにより、カスタマ網とプロバイダ網との境界においてカスタマ通信装置とエッジ通信装置とに対してＢＧＰの実装を不要として、負荷の増大を防止し、またカスタマ網のルーティングプロトコルとして、ＯＳＰＦプロトコルを使用することで、プロバイダ網との間でのマルチホーミングを構築可能となり、信頼性の向上が図れる。更に、単一ＯＳＰＦドメインで各カスタマ網を接続することが可能となるものである。

【００２５】

【発明の実施の形態】以下に、図面を参照しつつ本発明の実施の形態につき詳述する。図１は本発明によるエッジノードを用いて構築したＶＰＮ構成を説明するための概略システム構成図であり、図１６と同等部分は同一符号により示している。ここで提案されるＶＰＮ構築方式は、カスタマノード１１～１３，２１～２３，３１～３３からなるカスタマ網Ａ１～Ａ３と、コアノード４４，４５とエッジノード４１～４３とからなるプロバイダ網Ｃ１とにより構成されている。

【００２６】図１におけるカスタマ網Ａ１、カスタマ網Ａ２、カスタマ網Ａ３は、プロバイダ網Ｃ１の境界で

の、すなわちトンネル５１や５２の両端に位置するエッジノードでのカプセル化処理によるトンネリングにより、ＶＰＮを構築している。従って、カスタマ網Ａ１～Ａ３は同一のＡＳ（Autonomous System ）に属し、同一のＩＧＰｓ（Interior Gateway Protocols）、例えば、ＲＩＰ（Routing Information Protocol）、ＯＳＰＦ（Open Shortest Path First）により、カスタマノードのトポロジデータベースを更新／管理することができる。尚、本例では、ＩＧＰｓとしてＯＳＰＦを使用するものとしている。

【００２７】エッジノード４１～４３の各々のカスタマ網側は、接続されたカスタマ網で使われているＯＳＰＦプロトコルの終端処理が可能であり、よって図１に示すように、カスタマ網Ａ１～Ａ３はＣ（Customer）－ＯＳＰＦが使用可能であり、プロバイダ網Ｃ１はＶＲ（VPN ROUTING ）－ＯＳＰＦが使用可能であり、図１３に示したようにカスタマ網とプロバイダ網との間のインタフェース部で使用されていたＥＢＧＰを使用する必要がなくなる。すなわち、カスタマ網側のＣ－ＯＳＰＦ制御パケットは、プロバイダ網内では、一般のＩＰパケットとして転送され、トンネルとなるのである。各Ｃ－ＯＳＰＦはプロバイダ網内のＶＲ－ＯＳＰＦの存在に気付かないということであり、つまりは、各Ｃ－ＯＳＰＦは同じＯＳＰＦドメインに属することになる。これ等を実現する機能として、エッジノードにおいて、終端機能とＶＲテーブル情報の更新機能とを設けるものである。

【００２８】また、ＯＳＰＦでは、複数のリンクに対して異なるメトリック値を設定しておき、メトリック値が、例えば小なるリンクを優先的に選択する、いわゆるマルチホーミングが使用可能であるので、カスタマ網とプロバイダ網との間でこのマルチホーミングを構築可能として、信頼性の向上を図り得るのである。

【００２９】図２は本発明の実施例を示すシステム概略図であり、図１と同等部分は同一符号にて示している。尚、図２では、簡単化のためにコアノードは省略して示している。図２に示すように、カスタマ網Ａ１のカスタマノード１１～１３のプライベートＩＰ（Internet Protocol ）アドレスは“ａａ”，“ａｂ”，“ａｃ”とし、またカスタマ網Ａ２のカスタマノード２１～２３のプライベートＩＰアドレスは“ｂａ”，“ｂｂ”，“ｂｃ”とし、更にカスタマ網Ａ３のカスタマノード３１～３３のプライベートＩＰアドレスは“ｃａ”，“ｃｂ”，“ｃｃ”とする。

【００３０】エッジノード４１～４３のプロバイダ網Ｃ１側のカプセルアドレスは“Ｅ１”～“Ｅ３”とする。そして、エッジノード４１のカスタマ網側のインタフェースのアドレス（プライベートＩＰアドレス）は“１１１”とし、エッジノード４２のカスタマ網側のインタフェースのＩＰアドレスは“１２１”とし、エッジノード４３のカスタマ網側のインタフェースのＩＰアドレスは“１３１”及び“１３２”とする。

【００３１】そして、本実施例では、前述のマルチホーミングのためのカスタマ網Ａ１内でのトポロジデータベース（ルーティングのためのルーティングテーブル）に対して、２つのプライベートＩＰアドレス“１１１”と“１２１”とを、予め提供しておくものとする。カスタマ網Ａ１内でのルーティングプロトコル（ＯＳＰＦ）において、この提供された２つのＩＰアドレス“１１１”，“１２１”を経路とするメトリック値の大小を、前者の経路の値がより小となるようにしておくことで、ＩＰアドレス“１１１”を経るルーティングであるＶＰＮトンネル５１が現用系として選択されるようにすることができる。

【００３２】図３は図２におけるエッジノードの概略ブロック図であり、カスタマ網からのパケットを終端処理する終端部１と、この終端部の動作制御やルーティングの制御をなす制御部（ＣＰＵ）２と、ＶＰＮ構築情報及びプロバイダ網に接続され予めカプセルアドレスが割り当てられたポートとカスタマ網の各ノードのＩＰアドレスとの対応情報を有するテーブル、すなわちＶＲテーブル３と、制御部の動作制御プログラム（ソフトウェア）を予め格納したＲＯＭ４と、カスタマ網及びプロバイダ網とのインタフェースをなすＩ／Ｆ部５，６とを有している。

【００３３】図４はエッジノード４１～４３が夫々有するルーティング制御のためのＶＲテーブルの概念図を示しており、ＶＲテーブルは同じＶＰＮ　ＩＤ（ＶＰＮ識別情報）を持っていてもそれが格納されるエッジノードによりその内容は相違しており、図４に示すように、エッジノード４１はＶＲ　ＩＤとして“１１”，“１２”，“１３”，……に夫々対応するＶＲテーブルを有しており、ＶＲ　ＩＤ“１１”の具体例（図２に対応）が図５に示されている。また、エッジノード４２はＶＲ　ＩＤとして“２１”，“２２”，“２３”，……に夫々対応するＶＲテーブルを有しており、ＶＲ　ＩＤ“２１”の具体例（図２に対応）が図６に示されている。更に、エッジノード４３はＶＲ　ＩＤとして“３１”，“３２”，“３３”，……に夫々対応するＶＲテーブルを有しており、ＶＲ　ＩＤ“３１”の具体例（図２に対応）が図７に示されている。

【００３４】これ等ＶＲテーブルはカスタマ網側インタフェース（ＩＮＦ）の関連付け情報を含んでおり、これはＩＰ－ＶＰＮサービスをプロバイダ網に申し込む際に登録されるもので、カスタマ網側でプライベートアドレスが使用できるようにするための不可欠な情報である（異なるカスタマ網で同じアドレスが存在し得る場合があり、この場合どのカスタマ網側インタフェースから入力されてきたかでＶＲテーブルを識別するものである）。また、Ｅｇｒｅｓｓ（出力）エッジノードのカスタマ側インタフェースの状態、つまりそのカプセル化ア

ドレスが有効であるかどうかの情報（ＯＫ／ＮＧ）をも含んでいる。

【００３５】更に、ＶＰＮ　ＩＤをも含んでいる。このＶＰＮ　ＩＤはそのＶＲテーブルを使用するカスタマに付与されたグローバルユニークな情報である。ＶＲテーブルは同じＶＰＮ　ＩＤを持っていても、それが格納されるエッジノードにより相違するものである（図４参照）。また、カプセル化アドレスの優先度をも含み、この優先度は先述したメトリック値に相当するものであって、優先度“１”（現用系）が“２”（予備系）よりも優先するものとする。

【００３６】図８は本発明の実施例の動作を示すシーケンス図であり、カスタマ網からのパケット転送時と、カスタマ網でのアドレス変更時と、メトリック小（現用系）のリンク断時との、各場合におけるものである。先ず、カスタマ網からのパケット転送時について、図９のフローチャートをも参照しつつ説明する。例えば、カスタマ網Ａ１のノード１２から他のカスタマ網Ａ２のノード２２へパケット転送要求があるとする（ステップＳ１）。このときのパケットは、図１０（Ａ）に示すように、そのヘッダ部分に、送信元アドレス／宛先アドレスとして、ａｂ／ｂｂが表記されている。

【００３７】カスタマ網Ａ１内でのＯＳＰＦルーティングプロトコルに従って当該パケットはノード１１を経て、メトリック値が小のリンクが自動的に選択されてエッジノード４１へ供給される。エッジノード４１では、終端処理が行われる。すなわち、そのパケットの転送先を解決すべく、先ずこのパケットが入力されてきたカスタマ網側インタフェースＩ１１から定まるＶＲテーブル（１１）を得る（ステップＳ２）。このＶＲテーブル（１１）から網内パケットに含ませるべきＶＰＮＩＤ（１）を得る（ステップＳ３）。

【００３８】次に、宛先プライベートアドレス（ｂｂ）と、Ｅｇｒｅｓｓエッジノードのカスタマ側ＩＮＦ状態（ＯＫ）を元に、カプセル化アドレス（Ｅ３）を解決し（ステップＳ４）、図１０（Ｂ）に示すように、ＶＰＮ　ＩＤと送信元カプセル化アドレス／宛先カプセル化アドレスであるＥ１／Ｅ３とがヘッダに付加されて、カプセル化が行われる（ステップＳ５）。このカプセル化されたパケットは対応する出力ＩＮＦ（プロバイダ網側）へ網内パケットとして転送される（ステップＳ６）。

【００３９】このカプセルを受信したエッジノード４３での動作を図１１のフローチャートに示している。エッジノード４３では、このカプセルを終端部１で受信して（ステップＳ１１）、当該網内パケット転送先を解決するために、先ず当該パケットが持つＶＰＮ　ＩＤを元に、ＶＲテーブル（３１）を得て、このＶＲテーブル（３１）内で、宛先プライベートＩＰアドレス（ｂｂ）を元に、対応する出力ＩＮＦ（Ｉ３１）を決定する（ステップＳ１２）。そして、図１０（Ｃ）に示すように、カプセル化アドレスとＶＰＮ　ＩＤとをヘッダから外して逆カプセル化を行い（ステップＳ１４）、送信する（ステップＳ１５）。

【００４０】カスタマ網内のアドレスが変更された場合の動作を、図１２のフローチャートを参照して説明する。あるカスタマ網のあるノードのＩＰアドレスが変更になると、その変更を通知するための制御パケットが網内で転送され（Hello プロトコル等を使用して）、対応するエッジノードにも送信される（ステップＳ２１）。

【００４１】この制御パケットのヘッダ部には、このパケットが制御パケットである旨を示す情報が予め付加されているので、この情報により終端部１は制御パケットの認識が可能であり、この制御パケットにのせられているアドレス変更の情報を解読して、ＶＲテーブルの内容の更新を行う（ステップＳ２２）。そして、プロバイダ網内におけるＶＲテーブルの情報の交換をなすための交換プロトコルを使用して、関連するエッジノードに対して、アドレス変更の通知を行う（ステップＳ２３）。

【００４２】現用トンネルに対応するインタフェースのリンク（メトリック値が小）が断となった場合における動作を、図１３のフローチャートを使用して説明する。図２に示したメトリック値が小のリンクが断になると、その障害を通知するための制御パケットが網内で転送される（Hello プロトコル等を使用して）ので、各カスタマノードでは、トポロジＤＢ（データベース）が更新される。

【００４３】このとき、障害リンクに接続されているエッジノード４１では、障害発生が検出され（ステップＳ３１）、ＶＲテーブルから断リンクに関連する情報が削除される（ステップＳ３２）。この場合の削除の方法としては、ＶＲテーブル内のＥｇｒｅｓｓ側のカスタマ網ＩＮＦ状態が、ＮＧに設定されることでなされる。これにより、トンネル５１に関する情報はテーブルから削除されたことと等価になる。そして、交換プロトコルにより関連するエッジノードに対して同様に削除通知の他に、メトリックの小なるリンクがアクティブになる旨の通知がなされる（ステップＳ３３）。

【００４４】次に、図１４のフローチャートを参照すると、図１１のステップＳ３３による通知を受けた場合（ステップＳ４１）、そのＶＲテーブルから断リンクに関する情報が削除される（ステップＳ４２）。同時に、メトリックの大なるリンクがアクティブになる旨の通知により、ＶＲテーブルに対して、このメトリッの大のリンクに関する情報が追加される（ステップＳ４３）。

【００４５】ここで、ＩＧＰｓとしてＯＳＰＦを想定した場合、現用系として使用したいエッジ通信網に対してメトリック値を小さく設定し、他方のメトリック値は大きく設定しておく（ＶＰＮのメトリック値には、プロバイダ網内の経路を反映する方式と、しない方式とが考えられるが、ここでは、プロバイダ網内の経路から算出さ

れるメトリック値はＶＰＮのメトリック値に反映しないこととする。従って、図２の様なマルチホーミング構成では、メトリック値に大差をつける必要はなく、大小の関係が成立すればよい）。

【００４６】カスタマ網内のアドレスやトポロジの変更に伴うＶＲテーブルの更新には、プロバイダ網内でＩＢＧＰを使う前述した方式と、集中型処理装置を介して更新する方式とが考えられる。図１５はこの集中型処理装置を使用した方式の例であり、図２と同等部分は同一符号にて示している。この例では、集中処理装置１００が一方のエッジノードからＶＰＮ構築情報をアップロードし、しかる後に関係するエッジノード内ＶＲテーブルにダウンロードすることが考えられる。

【００４７】

【発明の効果】本発明によれば、カスタマノードは、ＢＧＰをサポートする必要はなく、ＩＧＰのみでＶＰＮが構築できるという効果がある。また、カスタマノードが複数のエッジノードに接続されるマルチホーミング構成を、ＢＧＰを使用することなく構成することができ、ＶＰＮの信頼性を向上させることができるという効果もある。更に、ＯＳＰＦドメインの分断がなくなり、ＡＴＭやＦＲを使用した専用線上でＩＰ網を構築する方式のように、単一ＯＳＰＦドメインで、各カスタマ網を接続できるという意義は大である。

【図面の簡単な説明】

【図１】本発明の基本構成を示すシステムブロック図である。

【図２】本発明の実施例を示すシステムブロック図である。

【図３】本発明のエッジノードの機能を示す概略図である。

【図４】エッジノードにおけるＶＲテーブルとプロバイダ網側インタフェースとの関係を示す概念図である。

【図５】ＶＲテーブルの内容の一例を示す図である。

【図６】ＶＲテーブルの内容の一例を示す図である。

【図７】ＶＲテーブルの内容の一例を示す図である。

【図８】本発明の実施例の動作を説明するためのシーケンス図である。

【図９】本発明の実施例におけるパケット転送時の動作を示すフローである。

【図１０】カプセル化及び逆カプセル化を説明いるための図である。

【図１１】本発明の実施例におけるカプセル受信時の動作を示すフローである。

【図１２】本発明の実施例における制御パケット受信時の動作を示すフローである。

【図１３】本発明の実施例における現用リンク障害時の動作を示すフローである。

【図１４】本発明の実施例における予備リンクアクティブ時の動作を示すフローである。

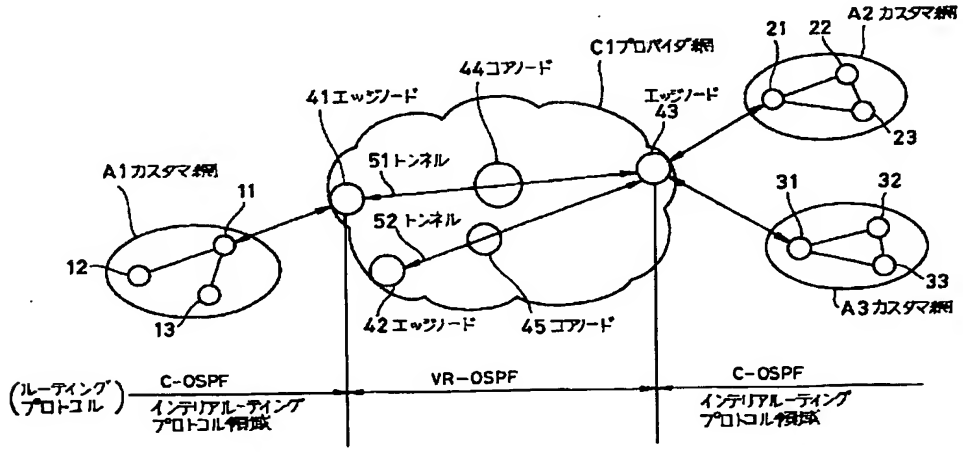
【図１５】本発明の他の実施例の概略システムブロック図である。

【図１６】従来技術を説明するための概略システムブロック図である。

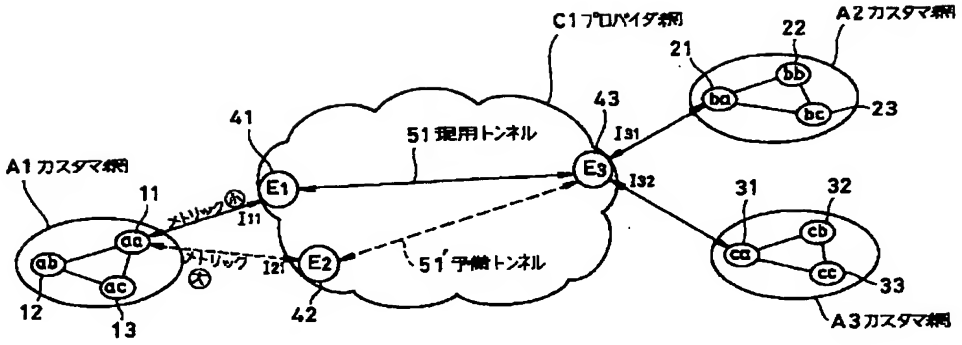
【符号の説明】

Ａ１～Ａ３　カスタマ網
Ｃ１　プロバイダ網
１　終端部
２　制御部
３　ＶＲテーブル
４　ＲＯＭ
５，６　インタフェース部
１１～１３，２２１～２３，
３１～３３　カスタマノード
４１～４３　エッジノード
５１　現用トンネル
５１′　予備トンネル
１００　集中処理装置

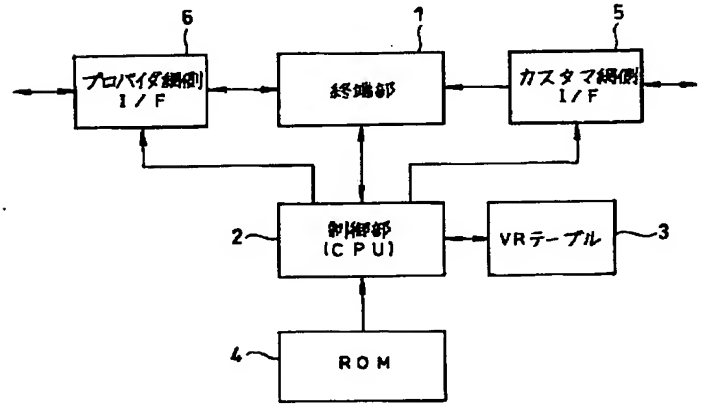
【図１】



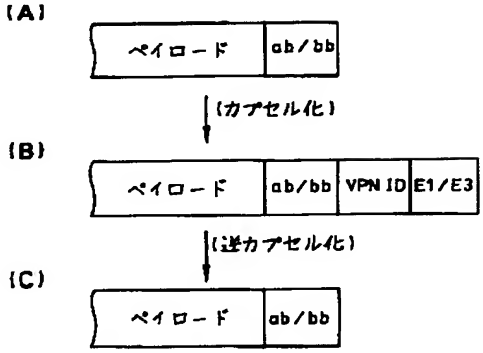
【図２】


C1プロバイダ網
A2カスタマ網
A1カスタマ網
A3カスタマ網
51 現用トンネル
51' 予備トンネル
E1
E2
E3
41
42
43
11
12
13
21
22
23
31
32
33
aa
ab
ac
ba
bb
bc
ca
cb
cc
I11
I21
I31
I32
メトリック小
メトリック大

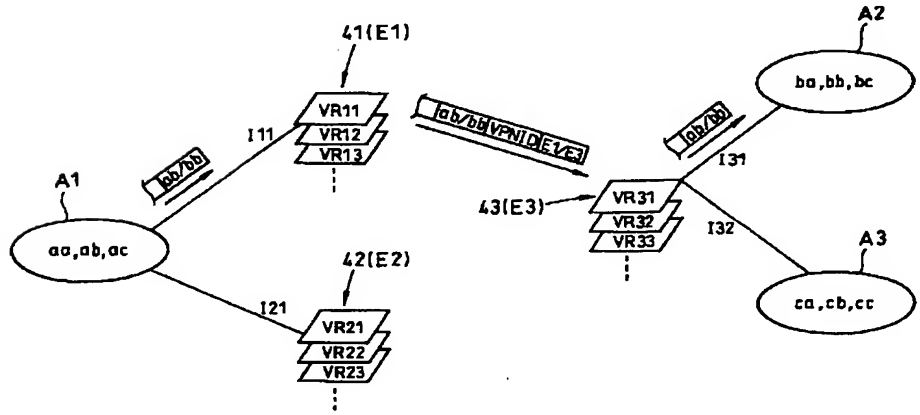
【図３】


6
1
5
プロバイダ網側 I/F
終端部
カスタマ網側 I/F
制御部 (CPU)
VRテーブル
ROM
2
3
4

【図１０】


(A)
ペイロード
ab/bb
(カプセル化)
(B)
ペイロード
ab/bb
VPN ID
E1/E3
(逆カプセル化)
(C)
ペイロード
ab/bb

【図４】


41(E1)
A2
ba,bb,bc
VR11
VR12
VR13
I11
ab/bb
ab/bb VPN ID E1/E3
ab/bb
I31
A1
aa,ab,ac
43(E3)
VR31
VR32
VR33
I32
A3
ca,cb,cc
42(E2)
I21
VR21
VR22
VR23

【図５】

41(E1)のVRテーブル

VRテーブルID	カスタマ側INF	VPN ID	宛先プライベートアドレス	カプセル化アドレス	Egressエッジのカスタマ側INF状態	VRからの出力INF	カプセル化アドレスの優先度
11	I11	1	a a	—	—	I11	—
			a b	—	—	I11	—
			a c	—	—	I11	—
			b a	E 3	OK/NG	プロバイダ側	1
			b b	E 3	OK/NG	プロバイダ側	1
			b c	E 3	OK/NG	プロバイダ側	1
			c a	E 3	OK/NG	プロバイダ側	1
			c b	E 3	OK/NG	プロバイダ側	1
			c c	E 3	OK/NG	プロバイダ側	1

【図６】

42(E2)のVRテーブル

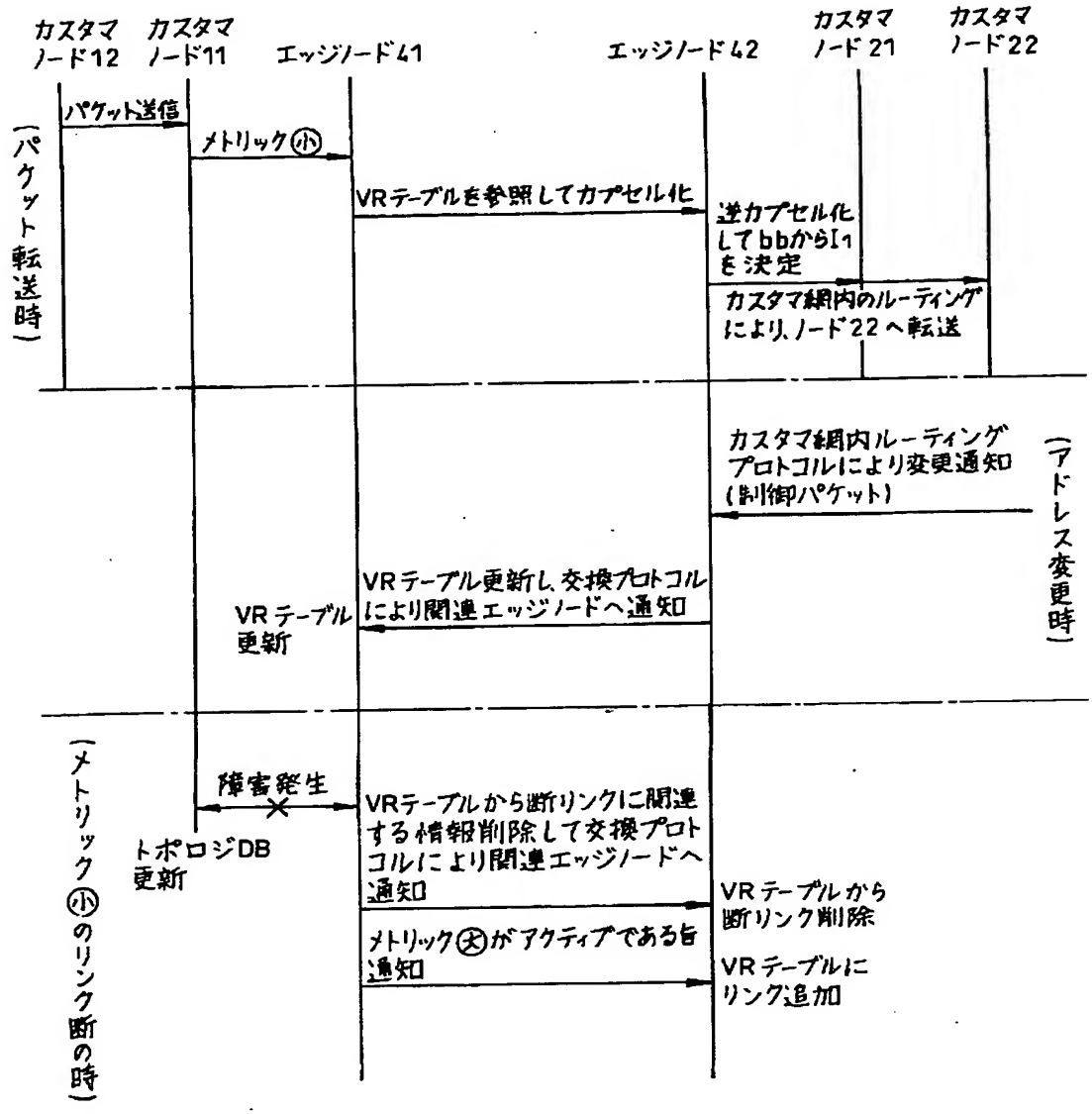
VRテーブルID	カスタマ側INF	VPN ID	宛先プライベートアドレス	カプセル化アドレス	Egressエッジのカスタマ側INF状態	VRからの出力INF	カプセル化アドレスの優先度
21	I21	1	a a	—	—	I21	—
			a b	—	—	I21	—
			a c	—	—	I21	—
			b a	E 3	OK/NG	プロバイダ側	1
			b b	E 3	OK/NG	プロバイダ側	1
			b c	E 3	OK/NG	プロバイダ側	1
			c a	E 3	OK/NG	プロバイダ側	1
			c b	E 3	OK/NG	プロバイダ側	1
			c c	E 3	OK/NG	プロバイダ側	1

【図７】

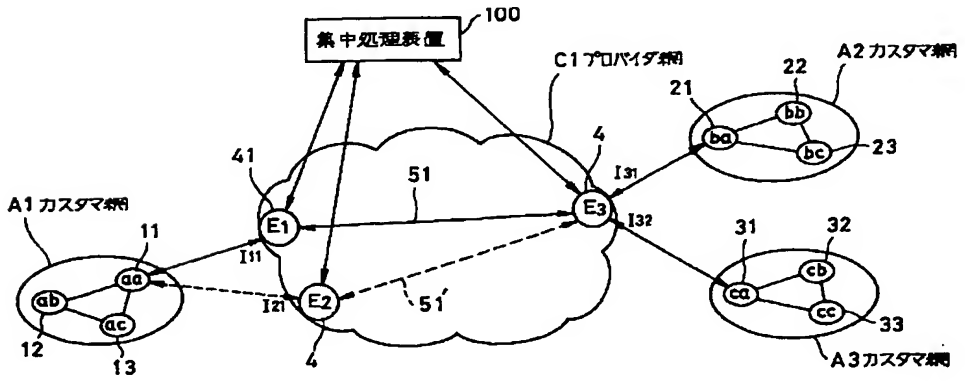
43(E3)のVRテーブル

VRテーブルID	カスタマ側INF	VPN ID	宛先プライベートアドレス	カプセル化アドレス	Egressエッジのカスタマ側INF状態	VRからの出力INF	カプセル化アドレスの優先度
31	I31	1	a a	E 1	OK/NG	プロバイダ側	1
	I32			E 2	OK/NG	プロバイダ側	2
			a b	E 1	OK/NG	プロバイダ側	1
				E 2	OK/NG	プロバイダ側	2
			a c	E 1	OK/NG	プロバイダ側	1
				E 2	OK/NG	プロバイダ側	2
			b a	—	—	I31	—
			b b	—	—	I31	—
			b c	—	—	I31	—
			c a	—	—	I32	—
			c b	—	—	I32	—
			c c	—	—	I32	—

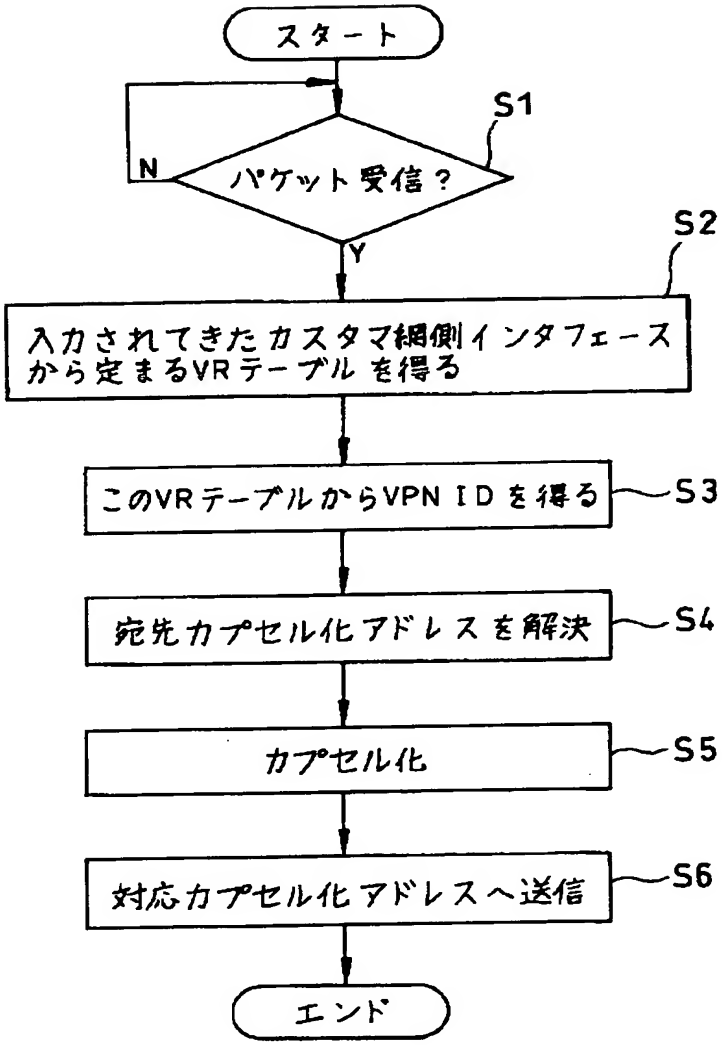
【図８】


カスタマノード12
カスタマノード11
エッジノード41
エッジノード42
カスタマノード21
カスタマノード22
（パケット転送時）
パケット送信
メトリック小
VRテーブルを参照してカプセル化
逆カプセル化してbbからI1を決定
カスタマ網内のルーティングにより、ノード22へ転送
（アドレス変更時）
カスタマ網内ルーティングプロトコルにより変更通知（制御パケット）
VRテーブル更新し、交換プロトコルにより関連エッジノードへ通知
VRテーブル更新
（メトリック小のリンク断の時）
障害発生
トポロジDB更新
VRテーブルから断リンクに関連する情報削除して交換プロトコルにより関連エッジノードへ通知
VRテーブルから断リンク削除
メトリック大がアクティブである旨通知
VRテーブルにリンク追加

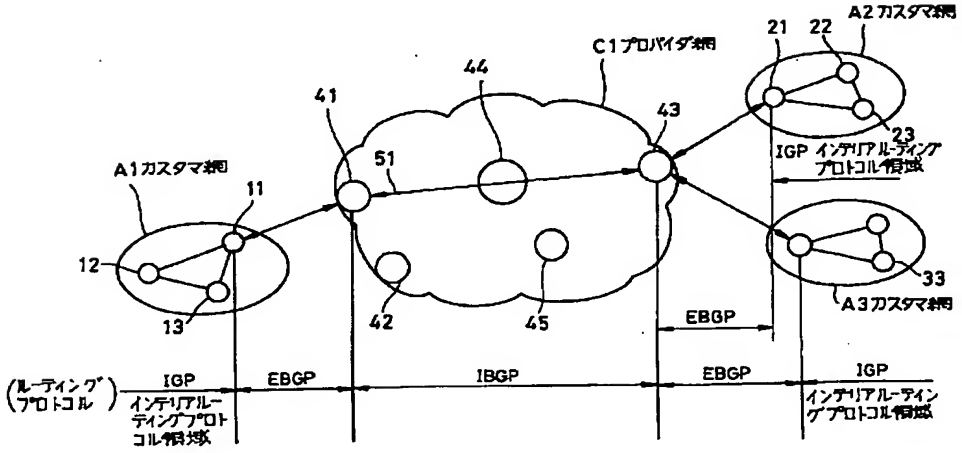
【図１５】


集中処理装置
100
C1プロバイダ網
A1カスタマ網
A2カスタマ網
A3カスタマ網
E1
E2
E3
41
4
51
51'
I11
I21
I31
I32
11
12
13
21
22
23
31
32
33
aa
ab
ac
ba
bb
bc
ca
cb
cc

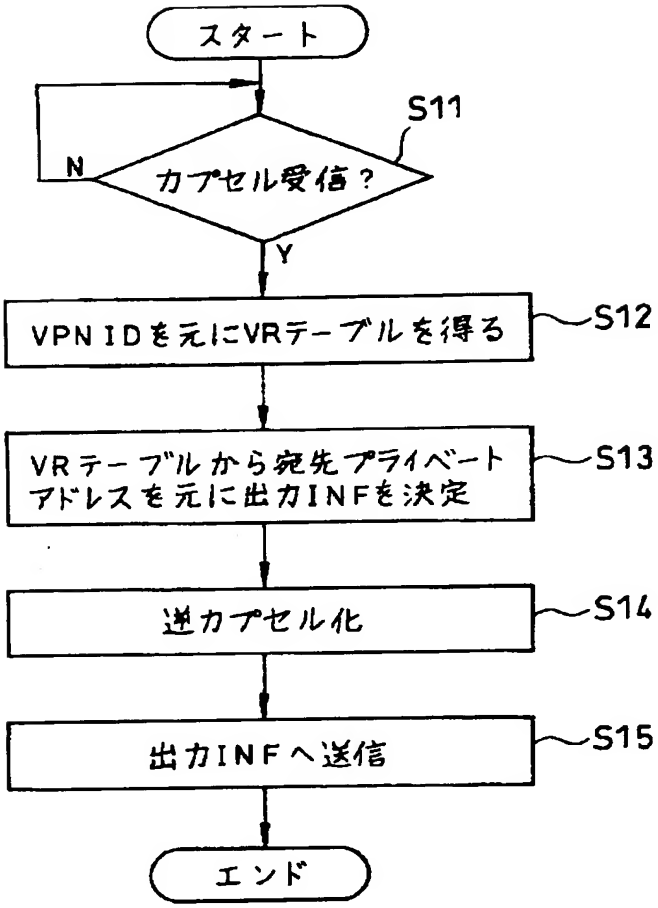
【図９】


スタート
S1
N
パケット受信？
Y
S2
入力されてきたカスタマ網側インタフェースから定まるVRテーブルを得る
このVRテーブルからVPN IDを得る
S3
宛先カプセル化アドレスを解決
S4
カプセル化
S5
対応カプセル化アドレスへ送信
S6
エンド

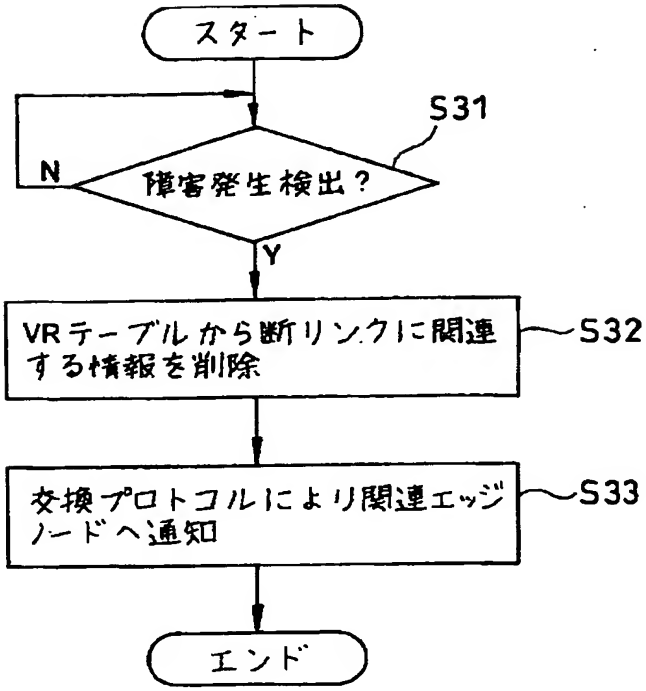
【図１６】


A2カスタマ網
21
22
C1プロバイダ網
44
41
43
23
IGP インテリアルーティングプロトコル領域
A1カスタマ網
11
51
12
33
13
42
45
A3カスタマ網
EBGP
(ルーティングプロトコル)
IGP
EBGP
IBGP
EBGP
IGP
インテリアルーティングプロトコル領域
インテリアルーティングプロトコル領域

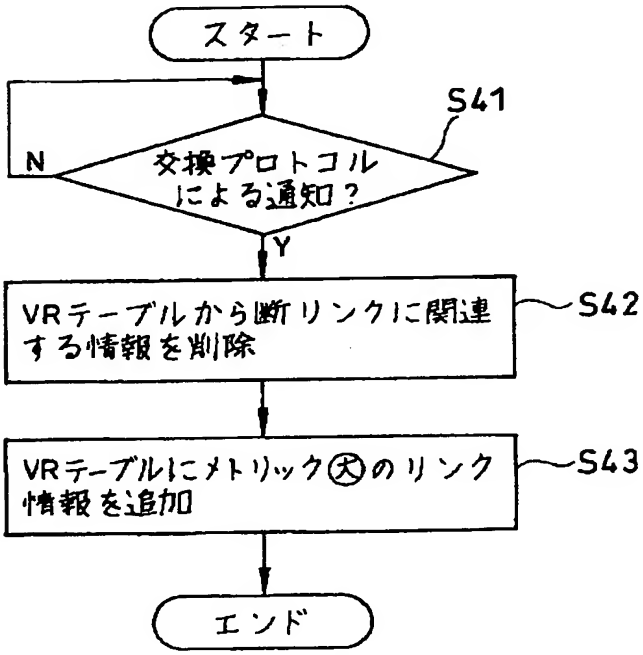
【図１１】


スタート
S11
N
カプセル受信？
Y
VPN IDを元にVRテーブルを得る
S12
VRテーブルから宛先プライベートアドレスを元に出力INFを決定
S13
逆カプセル化
S14
出力INFへ送信
S15
エンド

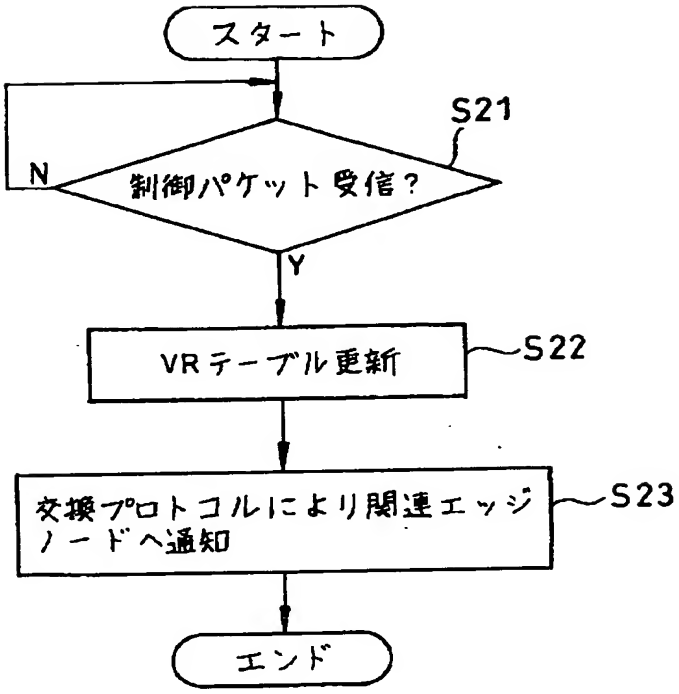
【図１３】


スタート
S31
N
障害発生検出？
Y
VRテーブルから断リンクに関連する情報を削除
S32
交換プロトコルにより関連エッジノードへ通知
S33
エンド

【図１４】


スタート
S41
N
交換プロトコルによる通知？
Y
VRテーブルから断リンクに関連する情報を削除
S42
VRテーブルにメトリック㊧のリンク情報を追加
S43
エンド

【図１２】


スタート
S21
N
制御パケット受信？
Y
VRテーブル更新
S22
交換プロトコルにより関連エッジノードへ通知
S23
エンド